

# 9520 Network Camera

## User Manual




# Before You Use This Product

The use of surveillance devices may be prohibited by law in your country. The Network Camera is not only a high-performance web-ready camera, but also can be part of a flexible surveillance system. It is the user's responsibility to ensure that the operation of such devices is legal before installing this unit for its intended use.

It is important to first verify that all contents received are complete according to the list in the "Package Contents" chapter. Take notice of the warnings in "Quick Installation" guide before the Network Camera is installed, then carefully read and follow the instructions in the "Installation" chapter to avoid damages due to faulty assembly and installation. This also ensures the product is used properly as intended.

The Network Camera is a network device and its use should be straightforward for those who have basic network knowledge. The "Troubleshooting" chapter in the Appendix provides remedies to the most common errors in set up and configuration. You should consult this chapter first if you run into a system error.

The Network Camera is designed for various applications including video sharing, general security/surveillance, etc. The "How to Use" chapter suggests ways to best utilize the Network Camera and ensure proper operations. For the creative and professional developers, the "URL Commands of The Network Camera" manual serves as a helpful reference to customize existing homepages or for integrating with the current web server.

For paragraphs preceded by  the reader should use caution to completely understand the warnings. Ignoring the warnings may result in serious hazards or injuries.

## Table of Contents

<b>Before You Use This Product .....</b>	<b>1</b>
<b>Table of Contents .....</b>	<b>2</b>
<b>Package Contents.....</b>	<b>3</b>
<b>Installation .....</b>	<b>3</b>
Hardware Installation .....	3
Network Installation .....	5
Software Installation .....	5
Initial Access to the Network Camera.....	6
How to Use .....	7
Installing plug-in .....	8
User Interface .....	9
System parameters.....	14
Security Settings .....	15
Network settings .....	17
DDNS .....	19
Access List.....	21
Audio and Video .....	22
Motion detection.....	28
Application.....	30
Recording .....	35
System log .....	38
Viewing system parameters .....	38
Maintenance .....	39
<b>Appendix.....</b>	<b>41</b>
A. Troubleshooting .....	41
B. Technical specifications .....	44

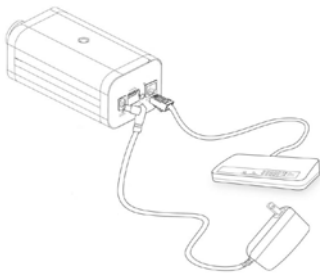
# Package Contents

- DVT9520
- Power adapter
- CD
- Quick Installation guide
- Accessory kit

## Installation

In this manual, "User" refers to whoever has access to the Network Camera, and "Administrator" refers to the person who can configure the Network Camera and grant user access to the camera.

### Hardware Installation



Please verify that your product package contains all the accessories listed in the foregoing Package Contents. The Ethernet cable should meet the specs of UTP Category 5 or better and not exceed 100 meters in length.



Connect the power adapter jack to the Network Camera before plugging in to the power socket. This will reduce the risk of accidental electric shock.

The 9520 Network Camera can be powered with either the 12VDC power supply (included) or with an 802.3af compliant Power Over Ethernet (PoE) source.

The Network camera can operate in two network modes, DHCP (default) or Fixed IP address.

Upon powering up, the LED will light up and the device will go through the booting process. The LED will be steady amber while booting up and acquiring an IP address. After getting an IP Address and completing the boot process, the LED will blink green every second to indicate proper operation (heartbeat).

## **Network Installation**

Make sure the network cable is firmly connected to both the camera and the network switch. After attaching the Ethernet cable, plug in the power adapter. If the LED blinks green, go to the next paragraph, "Software installation."

### ***Digital Input/Output***

This Network Camera provides a general I/O terminal block with one digital input and one digital output device control.

## **Software Installation**

Before installing your Network Camera, install the DVTel Device Wizard program included in the product CD-ROM. Refer to the Wizard manual for installation requirements.

Use the device Wizard to locate the Network Camera. There may be many Network Cameras in the local network. Users can differentiate the Network Cameras using the serial numbers (same as mac address). The serial number is printed on the labels on the carton and on the back of the Network Camera body. Please refer to the Wizard manual for details.

Once installation is complete, the Administrator should proceed to the "Initial Access to the Network Camera" section for necessary checks and configurations.

## Initial Access to the Network Camera

### *Configure IP address*

The Network Camera can be connected either before or immediately after software installation onto the Local Area Network. If DHCP is not used to assign an IP address, use the DVTel Device Wizard to assign the fixed IP address and complete the network settings, including the correct subnet mask and IP address of gateway and DNS. Ask your network administrator or Internet service provider for the detail information. By default, the Network Camera requires the Administrator to run installation every time it reboots. If the network settings are to remain unchanged, disable the Install option. Refer to "Network Settings" on the System Configuration page for details. If any setting is entered incorrectly and cannot proceed to setting up the Network Camera, restore the factory settings by following the steps in the "Troubleshooting" chapter of the Appendix.

### **Password Protection to prevent Unauthorized Access**

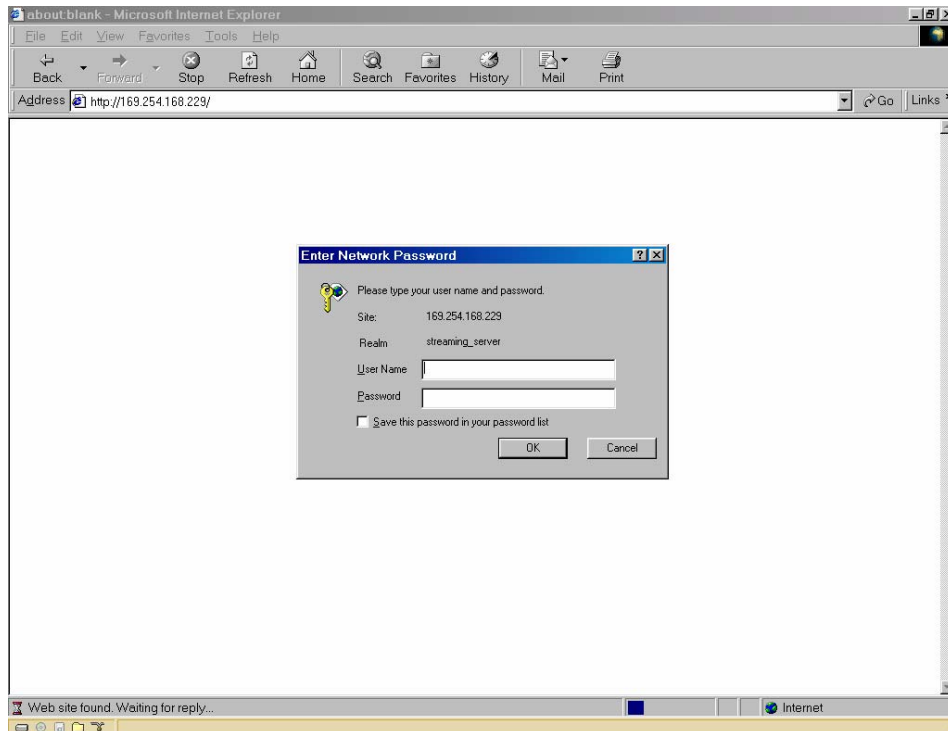
The default Administrator's password is blank and the Network Camera will not initially ask for any password. The Administrator should immediately implement a new password as a matter of prudent security practice. Once the Administrator's password is saved, the Network Camera will ask for the user's name and password before each access. The Administrator can set up a maximum of twenty (20) user accounts. Each user can access the Network Camera except to perform system configuration. Some critical functions are exclusive for the Administrator, such as system configuration, user administration, and software upgrades. The user name for the Administrator is permanently assigned as "root." Once the password is changed, the browser will display an authentication window to ask for the new password. **Once the password is set, there is no provision to recover the Administrator's password. The only option is to restore to the original factory default settings.**

## How to Use

A PC with a Windows operating system can use Internet Explorer (IE) to connect to the Network Camera. A plug-in will be installed into IE when it is connected for the first time. A PC with a Linux operating system can connect to the camera using a browser like Firefox. QuickTime must first be installed to view streaming.


## Authentication

After opening the Web browser and typing in the URL of the Network Camera, a dialogue window pops up requesting a username and password. Upon successful authentication, the following figure is displayed:



The foreground is the login window and the background shows the message if authentication fails. The user may check the option box to save the password for future convenience. This option is not available to the Administrator for obvious reasons.

## Installing plug-in

For initial access to the Network Camera in Windows, the web browser may prompt for permission to install a new plug-in for the Network Camera when using Internet Explorer. Permission request depends on the Internet security settings of the user's PC or notebook. If the highest security level is set, the computer may prohibit any installation and execution attempt. This plug-in, which has a registered digital certificate, is used to display the video in the browser. Users may click on  to proceed. If the web browser does not allow the user to continue to install, check the Internet security option and lower the security levels, or contact your IT or networking supervisor for help.



# User Interface

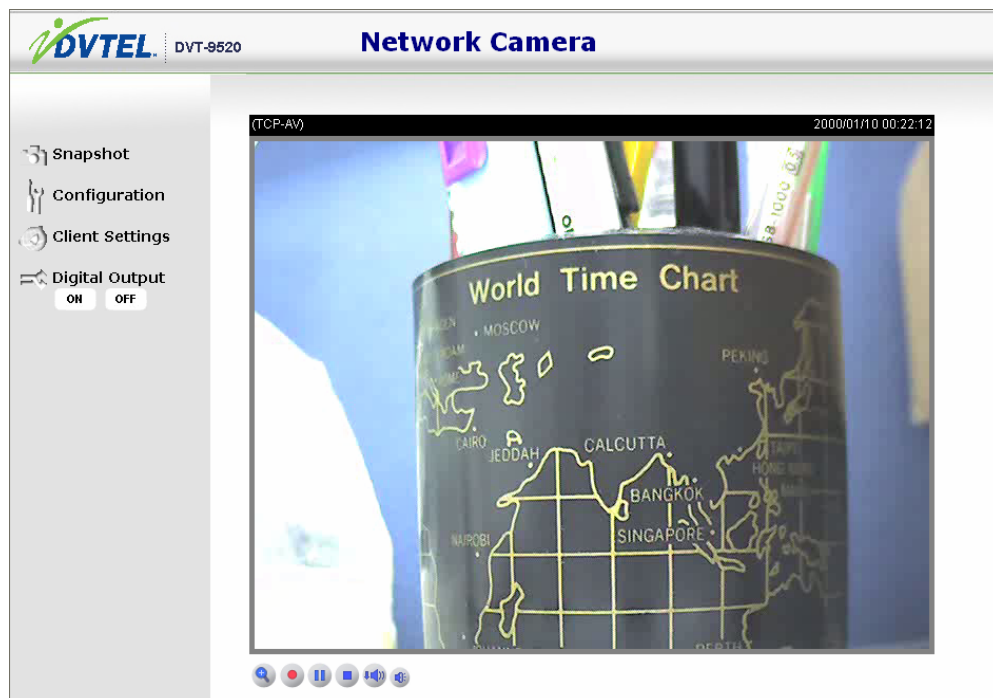
## Main Screen with Camera View

The main page layout has two parts:

- **Configuration functions:** The camera can be configured using these user interfaces.
- **Camera View:** What the camera sees.

Click on the configuration link to the left of the image window to enter the configuration page.

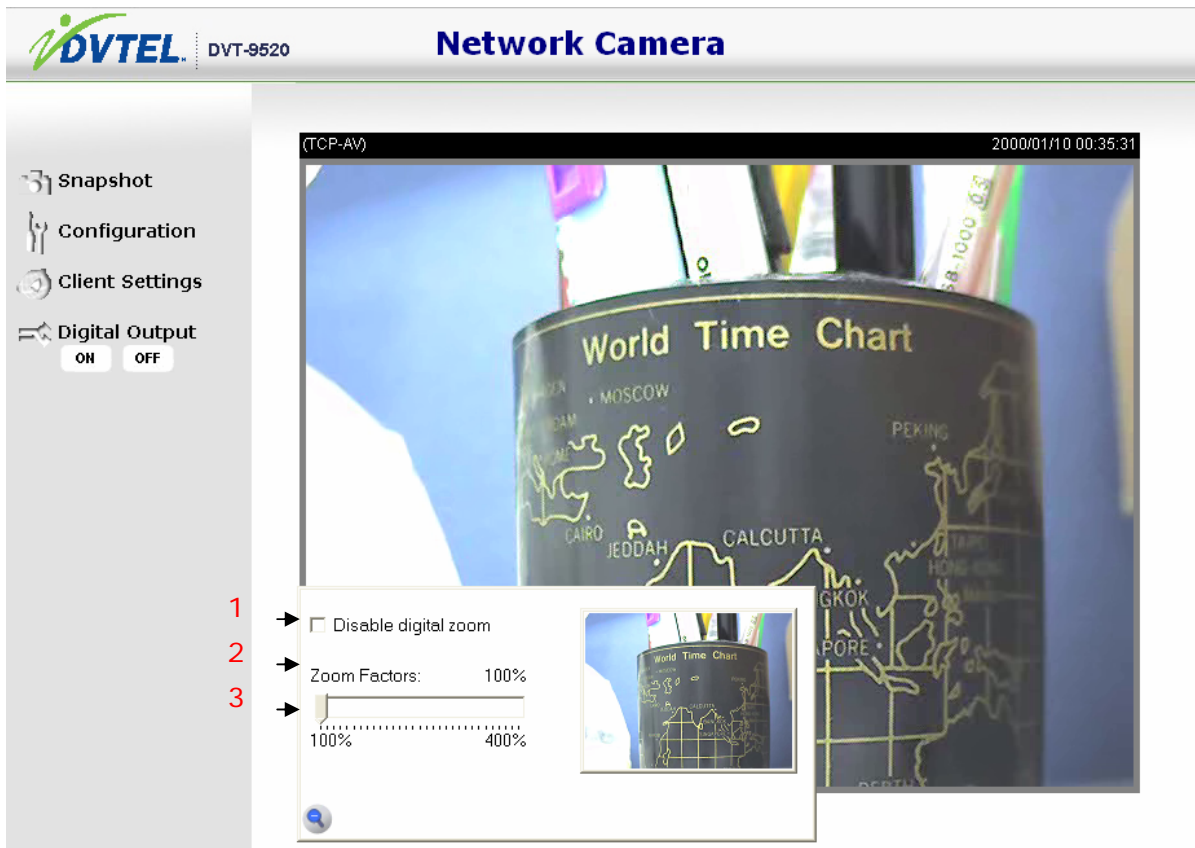
This is the layout in IE when it is streaming MPEG-4 video:




This function will be a little different when it is streaming JPEG video. Only digital zoom and the record button are supported.

## Digital Zoom

Click on the magnifier icon under the camera view. The digital zoom control panel is shown. Uncheck "Disable digital zoom" and use the slider control to change the zoom settings.



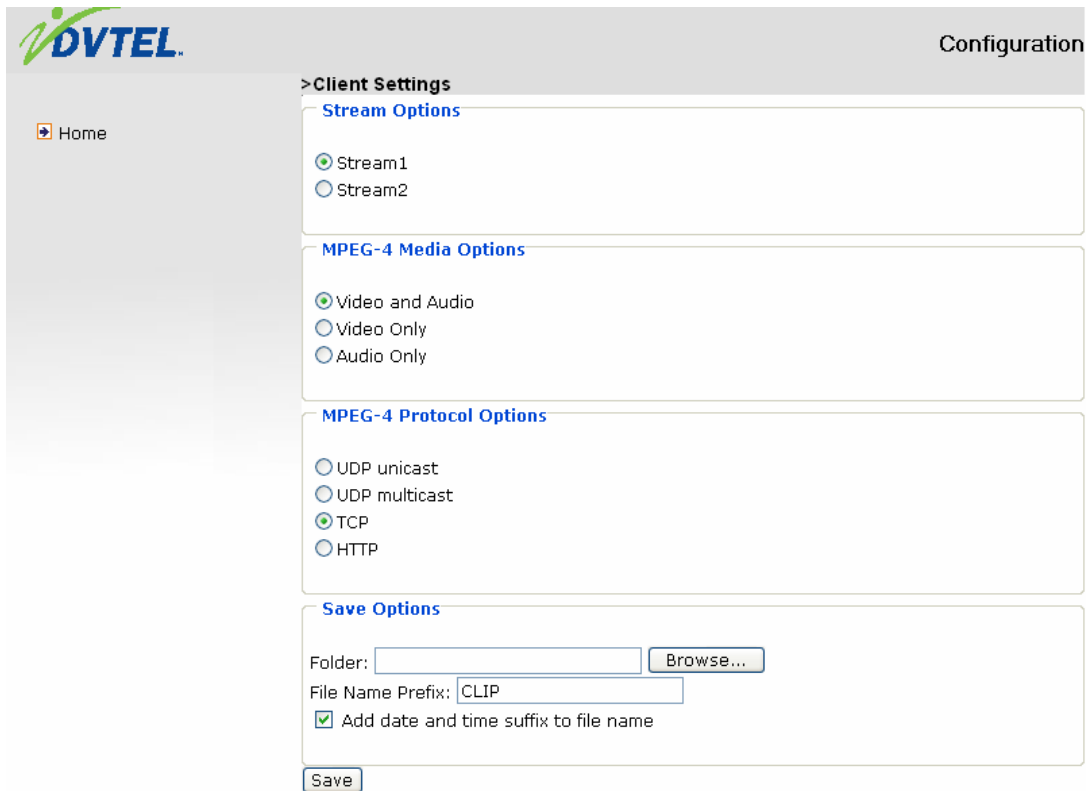
## MP4 Recording

Click on the red circle button  on the plug-in to start MP4 recording. You can set the related options in the client setting page.

## Snapshot

Click on "Snapshot." The web browser will pop up a new window to show the snapshot. Users can point at the snapshot and click the right button of mouse to save it.

## Client settings



The screenshot shows the DVTEL Configuration interface. On the left is a sidebar with a 'Home' link. The main area is titled 'Client Settings' and contains four sections: 'Stream Options' with radio buttons for 'Stream1' (selected) and 'Stream2'; 'MPEG-4 Media Options' with radio buttons for 'Video and Audio' (selected), 'Video Only', and 'Audio Only'; 'MPEG-4 Protocol Options' with radio buttons for 'UDP unicast', 'UDP multicast', 'TCP' (selected), and 'HTTP'; and 'Save Options' which includes a 'Folder:' text box with a 'Browse...' button, a 'File Name Prefix:' text box containing 'CLIP', a checked checkbox for 'Add date and time suffix to file name', and a 'Save' button at the bottom.

There are four settings for the client side in IE. The first option is “**Stream Options**” for users to determine which stream is to be viewed. This product supports dual-streams. The second one is “**MPEG-4 Media Options**” for users to determine which media is to be streaming under MPEG-4 mode. The third one is “**MPEG-4 Protocol Options**” which provides options on the connection protocol between client and server. There are four protocol choices to optimize your usage – UDP unicast, UDP multicast, TCP and HTTP:

The **UDP unicast** protocol allows for more real-time audio and video streams. However, some packets may be lost due to network burst traffic and images may be obscured. The **UDP multicast** protocol allows the saving of server bandwidth while serving multiple clients at the same time.

The **TCP** protocol allows for less packet loss and produces a more accurate video display. The downside with this protocol is that the real-time effect is worse than that with the UDP protocol.

The **HTTP** protocol allows the same quality as TCP protocol and the user doesn't need

to open a specific port to stream under some network environments.

If there are no special network requirements, UDP unicast protocol is recommended. Generally, the client's choice will be in the order of UDP multicast → UDP unicast → TCP → HTTP. After the Network Camera is connected successfully, "Protocol Option" will indicate the selected protocol. The selected protocol will be recorded in the user's PC and will be used for the next connection. If the network environment is changed, or the user wants to let the web browser detect again, manually select the UDP protocol, save, and return HOME to re-connect.

The fourth setting is "**Save Options.**" Users can specify the recording folder and file name prefix and suffix here.

## Digital output

Click "**ON**"; the digital output of the Network Camera is triggered. Or, clicking "**OFF**" can let the digital output turn into normal state.

## Administration

Only the Administrator can access the system configuration. Each category in the left column will be explained in the following pages. The bold text represents the specific phrases on the Option pages. The Administrator may type the URL below the figure to directly enter the frame page of configuration. If the Administrator also wants to set certain options through the URL, read the reference appendix for details.

The screenshot shows the DVTEL Configuration interface. On the left is a navigation menu with options: Home, System, Security, Network, DDNS, Access list, Audio and video, Motion detection, Application, Recording, System log, View parameters, and Maintenance. The main content area is titled 'Configuration' and contains three sections: 'System', 'System Time', and 'DI and DO'. The 'System' section has a 'Host name' field set to 'Network Camera' and a checkbox for 'Turn off the LED indicator'. The 'System Time' section has a 'Time zone' dropdown set to 'GMT+08:00 Beijing, Chongqing, Hong Kong, Kuala Lumpur, Singapore, Taipei', and three radio buttons for time synchronization: 'Keep current date and time' (selected), 'Sync with computer time' (with PC date and time fields), and 'Manual' (with Date and Time fields). There is also an 'Automatic' option with an 'NTP server' field and an 'Update interval' dropdown set to 'One hour'. The 'DI and DO' section has two status indicators: 'Digital input: normal status is Low' and 'Digital output: normal status is Open'. A 'Save' button is at the bottom.

Version: 0100b

<url> <http://<Network Camera>/setup/system.html>

<Network Camera> is the domain name or original IP address of the Network Camera.

## System parameters

**Host name:** The text displays the title at the top of the main page.

**Turn off the LED indicator:** Check this option to shut off the LED on the rear. It can prevent the camera's operation from being noticed.

**Time zone:** Adjust the time to that of the time-servers for local settings.

**Keep current date and time:** Click on this to reserve the current date and time of the Network Camera. An internal real-time clock maintains the date and time even if the system's power is turned off.

**Sync with computer time:** Synchronizes the date and time of the Network Camera with the local computer. The read-only date and time of the PC is displayed as updated.

**Manual:** Adjust the date and time according to what is entered by the Administrator. Notice the format in the related fields while completing the entry.


**Automatic:** Synchronize with the NTP server over the Internet whenever the Network Camera starts up. It will fail if the assigned time-server cannot be reached.

**NTP server:** Assign the IP address or domain name of the time-server. Leaving the text box blank connects the Network Camera to the default time-servers.

**Update interval:** Select hourly, daily, weekly, or monthly updates with the time on the NTP server.

**Digital input:** Select High or Low to define normal status of the digital input. The current status is also shown.

**Digital output:** Select Grounded or Open to define normal status of the digital output. The current status is also shown.

Remember to click on  to immediately validate the changes. Otherwise, the correct time will not be synchronized.

# Security Settings

## ***Password Protection***

The Network Camera is shipped without a password by default. This means that everyone can access the Network Camera and the configuration as long as the IP address is known. **It is necessary to assign a password if the Network Camera is intended to be accessed by others.**

**Root password (section 1):** To enable password protection, enter a password for the Root User. Change the Administrator's password by typing in the new password identically in both text boxes. The entries will be displayed as asterisks for security purposes. After pressing , the web browser will ask the Administrator for the new password for access.

**Add user (section 2):** Type the new username and password and press  to insert the new user. The new user will be displayed in the username list. There is a maximum of twenty user accounts. There are two kinds of authentication: Administrator and Operator. Administrator can fully control the camera operation. The operator's can view, listen and talk to cameras, and control the di/do of the camera. Network Cameras can provide twenty accounts.

**Manage user (section 3):** Pull down the user list to find the user's name and press  to delete the selected user. Or, edit the password or authentication of the selected user and press  to take effect.

## &gt;Security

- Home
- System
- Security
- Network
- DDNS
- Access list
- Audio and video
- Motion detection
- Application
- Recording
- System log
- View parameters
- Maintenance

Version: 0100b

**Root password**

\* Blank root password will disable user authentication.

Root password:

Confirm root password:

1

**Add user**

User name:

User password:

Authentication:

- ☒ Administrator  
☐ Operator  
☐ Viewer

2

**Manage User**

User name:

User password:


Authentication:

- ☐ Administrator  
☐ Operator  
☐ Viewer

3



## Network settings

Any changes made on the Network type section will restart the system in order to validate the changes. Make sure every field is entered correctly before clicking .

### Network type

**LAN & PPPoE:** The default type is LAN. Select PPPoE if using ADSL.

**Get IP address automatically & Use fixed IP address:** The default status is “**Get IP address automatically.**” It can be tedious having to perform software installation whenever the Network Camera starts. Therefore, once the network settings (especially the IP address) have been entered correctly, select “**Use fixed IP address (Default IP address: 169.254.0.99)**” and the Network Camera will skip installation at the next boot. The Network Camera can automatically restart and operate normally after a power outage. Users can run IP installer to check the IP address assigned to the Network Camera if the IP address is forgotten or they may use the UPnP function provided by the Network Camera (MS Windows XP provides UPnP function at **My Network Place**).

**IP address:** This is necessary for network identification.

**Subnet mask:** This is used to determine if the destination is in the same subnet. The default value is “255.255.255.0.”

**Default router:** This is the gateway used to forward frames to destinations in a different subnet. An invalid router setting will fail the transmission to destinations in different subnets.

**Primary DNS:** The primary domain name server that translates hostnames into IP addresses.

**Secondary DNS:** Secondary domain name server that backups the Primary DNS.

**Primary WINS server:** The primary WINS server that maintains the database of computer name and IP address.

**Secondary WINS server:** The secondary WINS server that maintains the database of computer name and IP address.

**Enable UPnP presentation:** Enable the UPnP camera short cut.

**Enable UPnP port forwarding:** Enable UPnP port forwarding.

**PPPoE:** If using the PPPoE interface, fill the following settings from ISP.

**User name:** The login name of PPPoE account.

**Password:** The password of PPPoE account.

**Confirm password:** Input password again for confirmation.

## HTTP

**Authentication:** Supports basic and digest modes.

**Http port:** This may be changed from the default Port 80. Once the port is changed, the users must be notified of the change for the connection to be successful. For instance, when the Administrator changes the HTTP port of the Network Camera whose IP address is 192.168.0.100 from 80 to 8888, the users must type in the web browser "http://192.168.0.100:8888" instead of "http://192.168.0.100."

**Secondary Http port:** Supports alternate port to access HTTP server.

**Access name for stream 1:** This is the access URL of stream 1 for making a connection from client software when its codec type is JPEG.

**Access name for stream 2:** This is the access URL of stream 2 for making a connection from client software when its codec type is JPEG.

Use http://<ip address>:<http port>/<access name> to make connection.

## FTP

**FTP port:** This may be changed from the default port 21. The user can change this value from 1025 to 65535. After the change, the external FTP client program must change the server port of connection accordingly.

## RTSP Streaming

**Authentication:** Supports disable, basic and digest modes.

**Access name for stream 1:** This is the access URL of stream1 for making connection from client software when the codec type is MPEG-4.

**Access name for stream 2:** This is the access URL of stream 2 for making connection from client software when the codec type is MPEG-4.

Use rtsp://<ip address>/<access name> to make connection.

**RTSP port:** This may be changed from the default Port 554

**RTP port for video:** The video channel port for RTP. It must be even number.

**RTCP port for video:** The video channel port for RTCP. It must be the port number of video RTP plus 1.

**RTP port for audio:** The audio channel port for RTP. It must be an even number.

**RTCP port for audio:** The video channel port for RTCP. It must be the port number of video RTP plus 1.

Users can modify Multicast setting for stream1 and stream2.

**Always multicast:** Select this to always enable multicast.

**Multicast group address:** This is used by sources and the receivers to send and receive content.

**Multicast video port:** The video channel port for multicast. It must be an even number.

**Multicast RTCP video port:** The video channel port for multicast RTCP. It must be the port number of multicast video port plus 1.

**Multicast audio port:** The audio channel port for multicast. It must be an even number.

**Multicast RTCP audio port:** The audio channel port for multicast RTCP. It must be the port number of multicast audio port plus 1.

**Multicast TTL:** This specifies the number of routers (hops) that multicast traffic is permitted to pass through before expiring on the network.

## DDNS

**Enable DDNS:** This option turns on the DDNS function.


**Provider:** The provider list contains four hosts that provide DDNS services. Connect to the service provider's website to make sure the service charges.

**Host Name:** If the user wants to use DDNS service, this field must be filled. Please input the hostname that is registered in the DDNS server.

**Username/E-mail:** The username or e-mail field is necessary for logging in the DDNS server or notify the user of the new IP address. Note: when this field is input as "Username" the following field must be input as "Password."

**Password/Key:** Please input the password or key to get the DDNS service.

**Save:** Click on this button to save current settings for the DDNS service and UPnP function.



Configuration

>DDNS

Home

System

Security

Network

DDNS

Access list

Audio and video

Motion detection

Application

Recording

System log

View parameters

Maintenance

DDNS: Dynamic domain name service

☐ Enable DDNS

Provider

Dyndns.org(Dynamic)

Host name

User name

Password

Save

Version: 0100b

<url> <http://<Network Camera>/setup/ddns.html>

<Network Camera> is the domain name or original IP address of the Network Camera.

## Access List

The access list is used to control the access permission of clients by checking the client IP address.

There are two lists for permission control: **Allow List** and **Deny List**. Only those clients whose IP address is in the **Allow List** and not in the **Deny List** can connect to the Video Server or Network Camera for receiving the audio/video streams.

Both the **Allow List** and **Deny List** consist of a list of IP ranges. If you want to add a new IP address range, type the **Start IP Address** and **End IP Address** in the text boxes and click on the **Add** button. If you want to remove an existing IP address range, just select from the pull-down menu and click on the **Delete** button.

Both the Allow List and Deny List can have 10 entries.

The screenshot shows the DVTEL Configuration interface. On the left is a navigation menu with options: Home, System, Security, Network, DDNS, Access list (selected), Audio and video, Motion detection, Application, Recording, System log, View parameters, and Maintenance. The main content area is titled 'Configuration' and 'Access list'. It contains four sections: 1. 'Allow list' with input fields for 'Start IP address' and 'End IP address', and an 'Add' button. 2. 'Delete allow list' with a pull-down menu for 'Allow list' (showing '1.0.0.0 ~ 255.255.255.255') and a 'Delete' button. 3. 'Deny list' with input fields for 'Start IP address' and 'End IP address', and an 'Add' button. 4. 'Delete deny list' with a pull-down menu for 'Deny list' and a 'Delete' button. The version '0100b' is noted at the bottom left.

<url> <http://<Network Camera>/setup/accesslist.html>

<Network Camera> is the domain name or original IP address of the Network Camera.

## Audio and Video

This product supports dual-stream. It provides two settings for video streams, but only one setting for audio.

### Video Settings

**Video title:** The text string can be displayed on video

**Color:** Select either color or monochrome video display.

**Power line frequency:** The fluorescent light will flash according to the power line frequency that depends on local utility. Change the frequency setting to eliminate uncomfortable flash image when the light source is only fluorescent light.

### Video orientation

**Flip:** Vertically rotate the video.

**Mirror:** Horizontally rotate the video. Check both options if the Network Camera is installed upside down.

**White balance:** Adjust the value for best color temperature.

**Maximum Exposure Time:** Adjust the maximum exposure time in different environments.

**Overlay title and time stamp on video:** When checked, the title is shown on video.

Note: There are different video quality settings for stream1 and stream2.

**Mode:** It can be MPEG-4 or JPEG. If MPEG-4 is selected, it is streamed in RTSP protocol. If JPEG is selected, it is streamed in server push mode.

**Frame Size:** For both MPEG-4 and JPEG, there are three options: 176x144, 320x240, and 640x480.

There are three dependent parameters provided in MPEG-4 mode for video performance adjustment:

**Intra frame period:** The interval of intra frame.

**Max frame rate:** This limits the maximal refresh frame rate, which can be combined with the video quality to optimize bandwidth utilization and video quality. Choose “**Constant bit rate.**” If the user wants to fix the bandwidth utilization regardless of the video quality, choose “**Fixed quality**” and select the desired bandwidth. The video quality may be poor due to the sending of maximal frame rate within the limited

bandwidth when images are moving rapidly. Consequently, to ensure detailed video quality (quantization rate) regardless of the network, it will utilize more bandwidth to send the maximal frames when images change drastically.

In JPEG mode, users can set **"Max frame rate"** and **"Video quality"** to adjust the video performance.

## Audio settings

Use **"Switch"**, **"Internal"**, or **"Microphone"** to set up the source of audio input and **"Mute"** To turn off audio

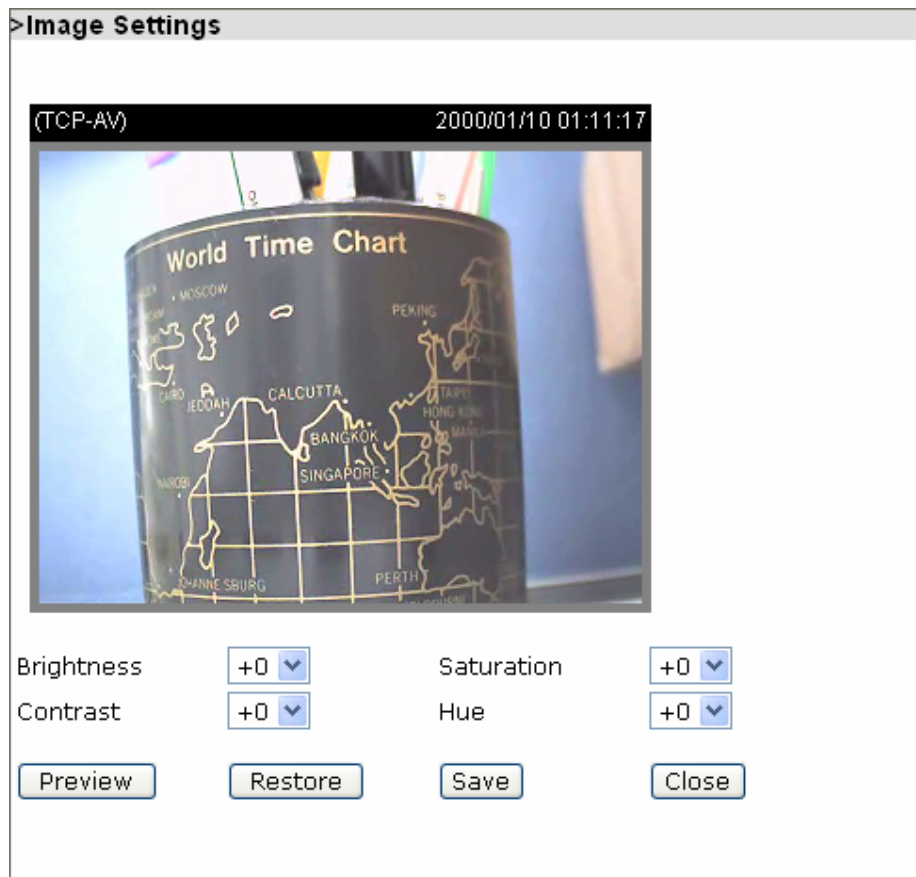
**Internal microphone input gain:** Modify the gain of the internal audio input.

**Audio type:** Select audio codec **"AAC"** or **"GSM-AMR"** and the bit rate.

<url> *http://<Network Camera>/setup/audiovideo.htm*

<Network Camera> is the domain name or original IP address of the Network Camera.

## Image Settings




**Image settings** Click on this button to pop up another window to tune "**Brightness**", "**Contrast**", "**Hue**" and "**Saturation**" for video compensation. Each field has eleven (11) levels ranging from -5 to +5. In the "**Brightness**" and "**Contrast**" fields the value "0" indicates auto-tuning. The user may press **Preview** to fine tune the image. When the image is O.K., press **Save** to set the image settings. Click on **Restore** to recall the original settings without incorporating the changes.

## Optimizing Image Quality

Best performance generally equates to the fastest image refresh rate with the best video quality, at the lowest network bandwidth as possible. There are three factors for the MPEG-4 mode ("Maximum frame rate", "Constant bit rate", and "Fix quality") and the "Maximum frame rate" and "Fix quality" for the JPEG mode. These setting may be adjusted to provide the best image quality and/or frame rate for the specific network environment.





Configuration

- Home
- System
- Security
- Network
- DDNS
- Access list
- Audio and video
- Motion detection
- Application
- Recording
- System log
- View parameters
- Maintenance

Version: 0100b

### >Audio and video

#### Video settings

Video title:

Color:

Color ▼

Power line frequency:

60 Hz ▼

Video orientation:

☐ Flip
 ☐ Mirror

White balance:

Auto ▼

Maximum Exposure Time:

1/60 S ▼

☐ Overlay title and time stamp on video

Image Settings

Privacy mask

☒ Video quality settings for stream1
 

Mode:

MPEG-4 ▼

Frame size:

640x480 ▼

Maximum frame rate:

30 fps ▼

Intra frame period:

1 S ▼

Video quality

☐ Constant bit rate:

512 Kbps ▼

☒ Fixed quality:

Good ▼

☒ video quality settings for stream2
 

Mode:

MPEG-4 ▼

Frame size:

176x144 ▼

Maximum frame rate:

5 fps ▼

Intra frame period:

1 S ▼

Video quality

☒ Constant bit rate:

40 Kbps ▼

☐ Fixed quality:

Good ▼

### Best Real-time Images

To achieve the best real-time visual effect, the network bandwidth should be large enough to allow a transmission rate of greater than twenty (20) image frames per second. If the broadband network is over 1 mbps, set the "Constant bit rate" to 1000 kbps or 1200 kbps, or set "Fixed quality" at the highest quality. (The maximum frame rate is 30.) If your network bandwidth is more than 512 kbps, you can fix the bit rate according to your bandwidth and set the maximum frame rate to 30 fps. If the images vary dramatically in your environment, you may want to slow the maximum frame rate down to 20 fps in order to lower the rate of data transmission. This allows for better video quality, and the human eye cannot readily detect the differences between those of 20, 25, or 30 frames per second. If your network bandwidth is below 512 kbps, set the "Constant bit rate" according to your bandwidth and try to get the best performance by fine-tuning using "Maximum frame rate." In a slow network, greater frame rate results in blurred images. Video quality performance will vary somewhat due to the

number of users viewing on the network, even if the parameters have been initially finely tuned. Performance will also suffer due to poor connectivity because of the network's burst constraint.

### ***Best Quality Images***

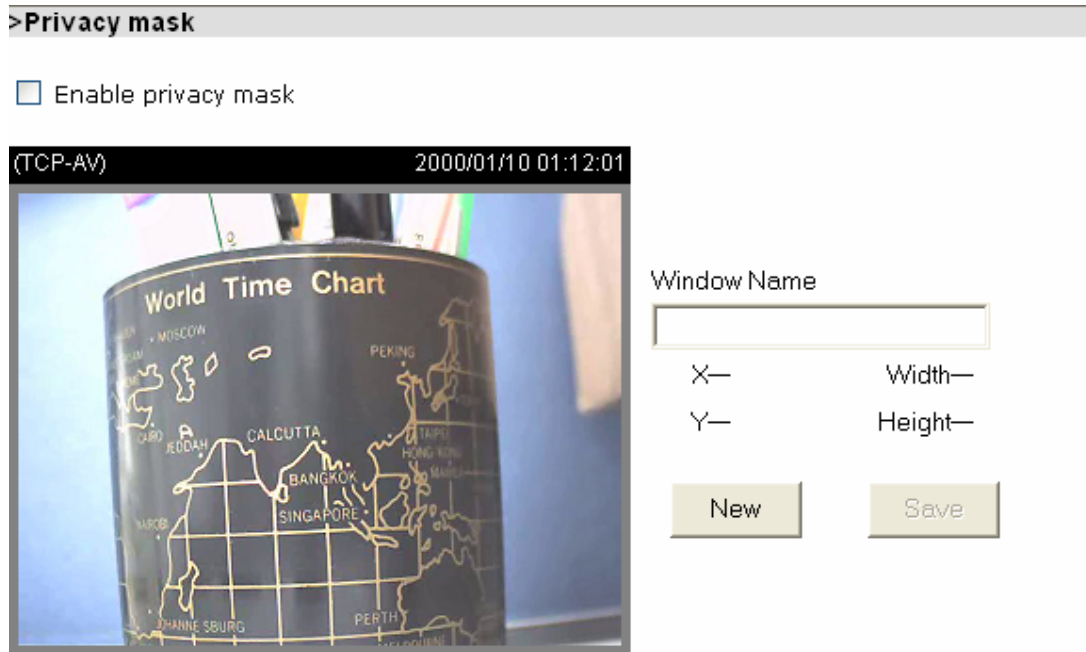
To have the best video quality, set "Fixed quality" at "Detailed" or "Excellent" and adjust the "Maximum frame rate" to match your network's bandwidth. If your network is slow and you receive "broken" images, go to the TCP or HTTP protocol in "MPEG-4 Protocol Options" and choose a more appropriate mode of transmission. The images may suffer a time delay due to a slower connection. The delay will also increase with added number of users.

### ***Somewhere between Real-time and best Quality Images***

If you have a broadband network, set "Fixed quality" at "Normal" or better, rather than setting "Constant bit rate." You can also fix the bandwidth according to your actual network speed and adjust the frame rate. Start from 30 fps down for best results but do not go below 15 fps. If the image qualities are not improved, select a lower bandwidth setting.

## Privacy Mask

Click on Privacy Mask button to bring up the privacy mask window.



Up to five privacy masks can be created. When enabled, users cannot view the blocked area under the privacy mask window.

**Enable privacy mask:** Check this option to turn on privacy mask.

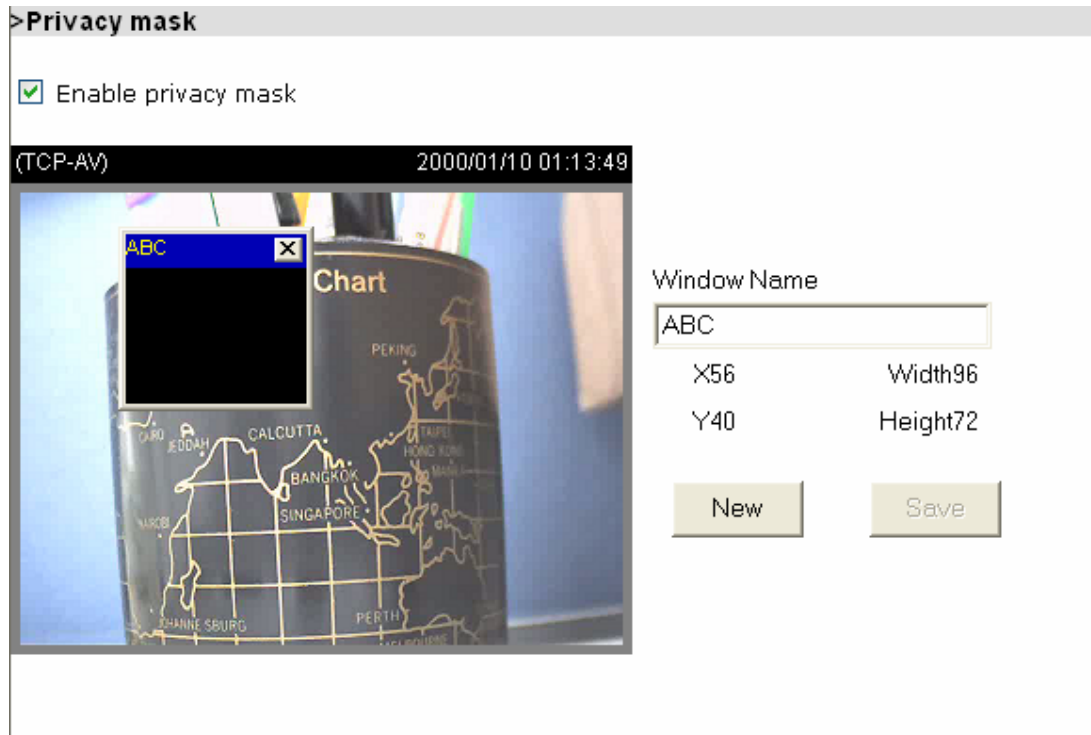
New

Click on this button to add a new window. A maximum of five windows can exist simultaneously. Use the mouse to click, hold, and drag the window frame to resize or click on the title bar to move. Click on the 'x' at the upper right-hand corner of the window to delete the window. Remember to save in order to validate the changes.

Save

Click on this button to save the related window settings.

**Window Name:** The text will show at the top of the window.



The above figure appears on the screen when **Save** is clicked and the privacy mask is enabled.

## Motion detection

**Enable motion detection:** Check this option to turn on motion detection.

**New** Click on this button to add a new window. At most three windows can exist simultaneously. Use the mouse to click, hold, and drag the window frame to resize or the title bar to move. Clicking on the 'x' at the upper right-hand corner of the window to delete the window. Remember to save in order to validate the changes.

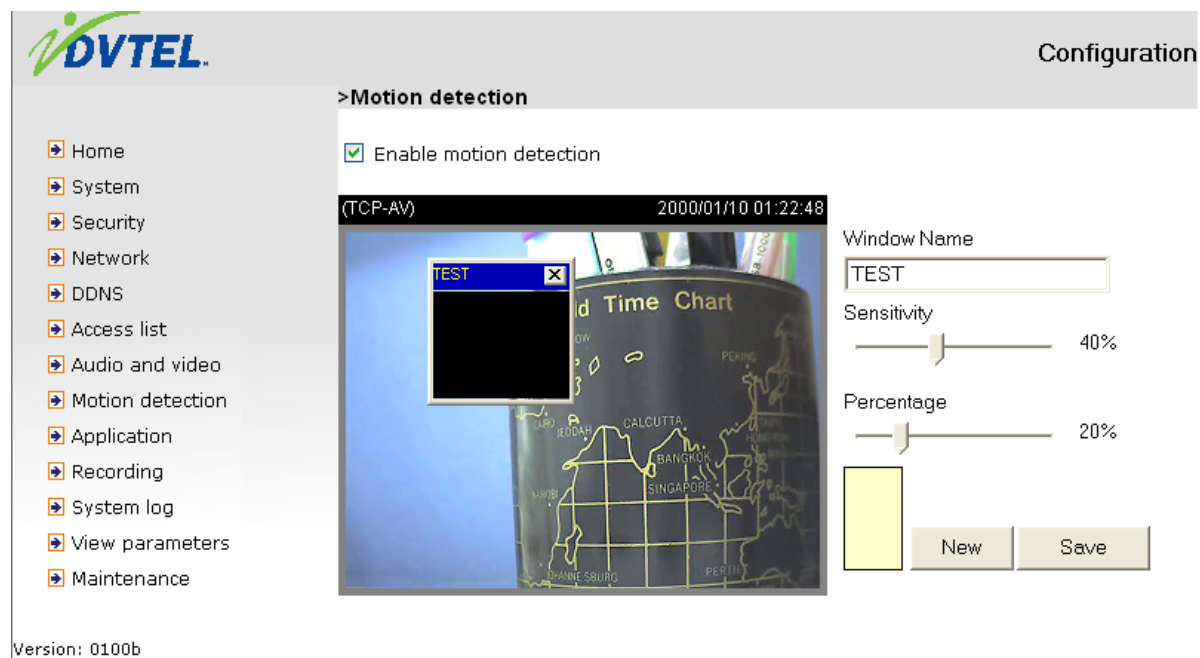
**Save** Click on this button to save the related window settings. A graphic bar will rise or fall depending on the image variation. A **green bar** means the image variation is under monitoring level and a **red bar** means the image variation is over monitoring level. When the bar goes red, the detected window will also be outlined in red. Going back to the homepage, the monitored window is hidden but the red frame shows when motion is detected.

**Window Name:** The name is shown at the top of the window.

**Sensitivity:** This sets the endurable difference between two sequential images.

**Percentage:** This sets the space ratio of moving objects in the monitoring window. Higher sensitivity and small percentage will allow easier motion detection.

Once Saved, the monitoring window will have a red outline and the graphic bar goes red when motion has been detected.



<url> <http://<Network Camera>/setup/motion.htm>

<Network Camera> is the domain name or original IP address of the Network Camera.

# Application

There are three sections in application page. They are **event**, **server** and **media**.

To add a new event, server, or media, click .


To delete a selected event, server, or media item, click .

To edit an item, click on the item name.

There can be a maximum of three events, a maximum of five servers, and a maximum of five media configurations.

Users can know the event name, status, weekly and time schedules, and trigger type in the event section. The server name, type and address/location are shown in server section. The current media free space, media name and type are shown in the media section. After adding a new media, the value of free space will be updated. Users cannot add media the size of which is larger than free space.

It is recommended that users first set servers and medias before setting events. The servers and medias selected in the event list cannot modified or deleted. First remove them from the event list if you want to delete or modify them. It is recommended that different media are used for different events. If the same media is used for different events and the events trigger almost simultaneously, the server for the second triggered event will not receive any media, there would be only notifications.


Configuration

- Home
- System
- Security
- Network
- DDNS
- Access list
- Audio and video
- Motion detection
- Application
- Recording
- System log
- View parameters
- Maintenance

>Application

**Event**

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger
<input type="button" value="Add"/>	<input type="button" value="▼"/>	<input type="button" value="Delete"/>								

**Server**

Name	Type	Address/Location
<input type="button" value="Add"/>	<input type="button" value="▼"/>	<input type="button" value="Delete"/>

**Media**

Media freespace: 9000KB

Name	Type
<input type="button" value="Add"/>	<input type="button" value="▼"/>
<input type="button" value="Delete"/>	

Version: 0100b

<url> *http://<Network Camera>/setup/application.htm*

<Network Camera> is the domain name or original IP address of the Network Camera.

## Event

**Event name:** The unique name for event.

**Enable this event:** Check to enable event.

**Priority:** The event with higher priority will be executed first.

**Delay second(s) before detecting next event:** The delay to check next event. It is used in motion detection and digital input trigger type.

There are four supported trigger types:

**Video motion detection:** Select the windows which need to be monitored.

**Periodic:** The event is triggered in specified intervals. The unit of trigger interval is minute.

**Digital input:** Used to monitor digital input.

**System boot:** The event is triggered when the system boots up.

The weekly and time schedules are provided:

**Sun ~ Sat:** Select the days of the week to perform the event.

**Time show Always:** You may also input the time interval.

If there are servers configured, the user can select them from “**Server name.**”

**Trigger DO:** Check this to trigger digital output for specific seconds when an event is triggered.

**Server name:** Check this to send the selected media when an event is triggered.

**Event**

Event name:

☐ Enable this event

Priority:

Delay for  seconds before detecting next event [For motion detection and digital input]

**Trigger**

☐ Video motion detection  
Detect motion in  
Note: Please configure [Motion detection](#) first

☐ Periodic  
Trigger every  minutes

☐ Digital input

☒ System boot

**Event schedule**

☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

**Time**

☒ Always

☐ From  to  [hh:mm]

**Action**

☐ Trigger D/O for  seconds

## Server

**Server name:** The unique name for a server.

There are four kinds of supported servers. They are **email server**, **FTP server**, **HTTP server** and **network storage**.

The following are the settings for an email server:

**Sender email address:** The sender's email address.

**Recipient email address:** The recipient's email address.

**Server address:** The domain name or IP address of the external email server.

**User name:** The granted user name on the external email server.

**Password:** The granted password on the external email server.



The following are the settings for an FTP server:

**Server address:** The domain name or IP address of the external FTP server.

**Server port:** This can be different than the default port 21. The user can change this value from 1025 to 65535.

**User name:** The granted user name on the external FTP server.

**Password:** The granted password on the external FTP server.

**Remote folder name:** The granted folder on the external FTP server. The string must conform to that of the external FTP server. Some FTP servers cannot accept a preceding slash symbol before the path without virtual path mapping. Refer to the instructions for the external FTP server for details. Note: The folder privilege must be open for upload.

**Passive Mode:** Check this to enable passive mode in transmission.

Below are the settings for an HTTP server:

**URL:** The URL to upload the media.

**User name:** The granted user name on the external HTTP server.

**Password:** The granted password on the external HTTP server.


Here are the settings for network storage. Only one network storage is supported.

**Network storage location:** The path to upload the media.

**Workgroup:** The workgroup for network storage.

**User name:** The granted user name on the network storage.

**Password:** The granted password on the network storage.

After inputting the setting of server, the user may click on  to test whether the setting is correct. The test result will appear in a pop-up window.

>Server

Server name:

Server type

☒ Email

Sender email address

Recipient email address

Server address

User name

Password

☐ FTP

Server address

Server port

User name

Password

Remote folder name

☒ Passive mode

☐ HTTP

URL

User name

Password

☐ Network storage

Network storage location

(for example: \\my\_nas\disk\folder)

Workgroup

User name

Password

Test Save Close

## Media

**Media name:** The unique name for the media.

There are three kinds of media: snapshot, video clip, and system log.

Snapshot settings:

**Source:** The source of stream, stream1 or stream2.

**Send Pre-event images:** The number of pre-event images.

**Send Post-event images:** The number of post-event images.

**File name prefix:** The prefix name to be added on the file name of the snapshot images.

**Add date and time suffix to file name:** Check this to add timing information as file name suffix.

Video clip settings:

**Source:** The source of stream, stream1 or stream2.

**Pre-event recording:** The interval of pre-event recording in seconds

**File name prefix:** The prefix name is added on the file name of the video clip.

There are two limitations for video clip files:

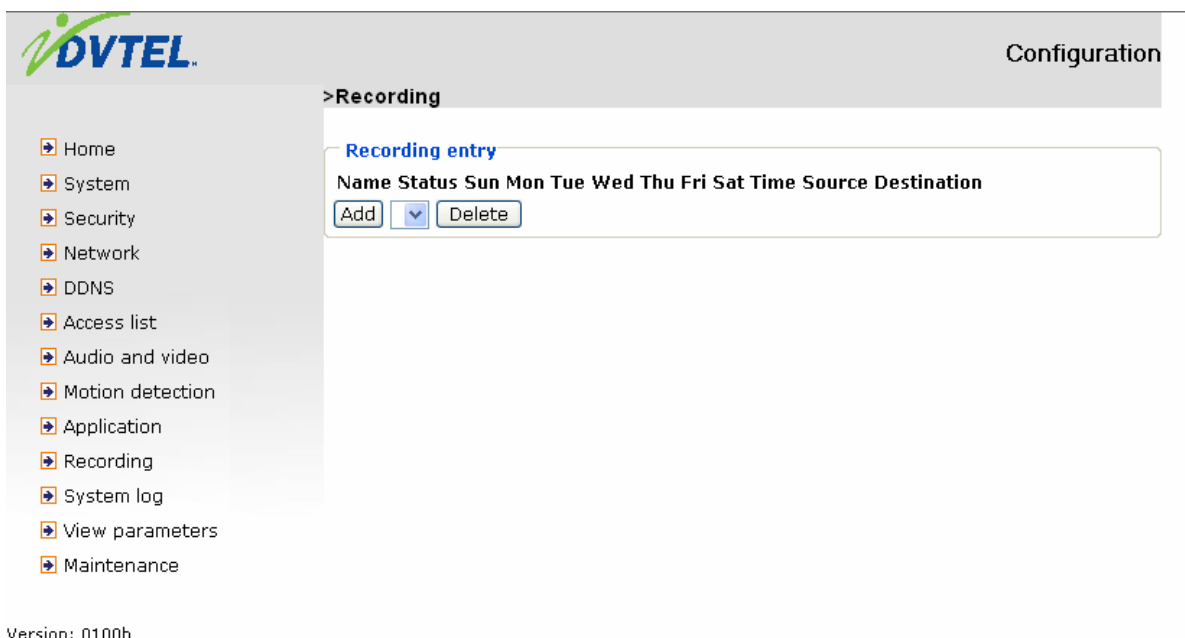
**Maximum duration:** The maximal recording file duration in seconds.

**Maximum file size:** The maximal file size to be generated.

The screenshot shows a web-based configuration interface for media recording. At the top, there is a tab labeled ">Media". Below the tab, there is a "Media name:" label followed by a text input field. Underneath, a section titled "Media type" contains three radio button options: "Snapshot", "Video Clip", and "System log". The "System log" option is currently selected. For the "Snapshot" option, the settings include a "Source:" dropdown menu set to "Stream1", two "Send" input fields (both set to "1") for "pre-event image(s) [0~7]" and "post-event image(s) [0~7]", a "File Name Prefix:" text input field, and an unchecked checkbox labeled "Add date and time suffix to file name". For the "Video Clip" option, the settings include a "Source:" dropdown menu set to "Stream1", a "Pre-event recording:" input field set to "0" with the unit "seconds [0~9]", a "Maximum duration:" input field set to "5" with the unit "seconds [1~10]", a "Maximum file size:" input field set to "500" with the unit "Kbytes [50~800]", and a "File Name Prefix:" text input field. At the bottom of the configuration area, there are "Save" and "Close" buttons.

## Recording

The Network camera supports recording to network storage. The operation of editing a recorded item is the same as the one in application page. Users can know the recording name, status, weekly and time schedule, stream source and destination of recording. There can be at most two recording entries. To do recording on network storage, first add a network storage server in the application page.



<url> *http://<Network Camera>/setup/recording.htm*

<Network Camera> is the domain name or original IP address of the Network Camera.

**Recording entry name:** The unique name for recording entry.

**Enable this recording:** Check this to enable this event.

**Priority:** The recording with higher priority will be executed first.

**Source:** The source of stream, stream1 or stream2.

The weekly and time schedules are provided.

**Sun ~ Sat:** Select the days of the week to perform the event.

**Time** shows “**Always**”, or you may input the time interval.

**Destination:** network storage server added by user.

**Total cycle recording size:** The total size for cycle recording in Kbytes.

**Size of each file for recording:** The single file size in Kbytes.

**File name prefix:** The prefix name is added on the file name of the recording.

Recording

Recording entry name:

☐ Enable this recording

Priority:

normal

Source:

Stream1

Recording schedule

☒ Sun
☒ Mon
☒ Tue
☒ Wed
☒ Thu
☒ Fri
☒ Sat

Time

☒ Always
☐ From 

00:00

 to 

24:00

 [hh:mm]

Destination

Server :

Note:

Please configure [Network storage](#) first

Total cycling recording size:

1000

Kbytes

Size of each file for recording:

200

Kbytes [200~6000]

File Name Prefix:

Save

Close

## Build a Security Application

The Administrator can use the built-in motion detection to monitor any movement and perform many useful security applications. To upload the snapshots, users can choose either email, FTP, HTTP, Network storage according to the user's needs. All server settings are in Server section on Application page. Refer to the definition section for detail configuration.

To enable motion based recording:

1. Click "**Configuration**" on the homepage.
2. Click "**Motion detection**" on the left column.
3. Check "**Enable motion detection.**"
4. Click on "**New**" to have a new window to monitor motion.
5. Type in a **name** to identify the new window.
6. Use the mouse to click, hold, and drag the window corner to resize or the title bar to move.
7. Fine-tune using the "**Sensitivity**" and "**Percentage**" fields to best suit the camera's environment. Higher "Sensitivity" detects slighter motion. Higher "Percentage" discriminates smaller objects.

- 37 -

8. Click on **"Save"** to enable the activity display. Green means the motion in the window is under the watermark set by Administrator, and red means it is over the watermark.
9. Click **"Application"** on the left column.
10. Add a server in the Server section.
11. Add a media with snapshot type in the Media section, and Set the number of pre-event and post-event images to be uploaded.
12. Add an event in the Event section:
  - Enter one event name and enable this event.
  - Check the weekdays as needed and set the time interval to monitor the motion detection every day.
  - Select the Trigger on Motion detection and Check the window name set in step 5.
  - Set the appropriate delay time to avoid continuous false alarms following the original event.
  - Check the server name set in Step 10 and select the media name set in Step 11.
13. Click **"Save"** to validate.

## System log

The Network camera support log the system messages on remote server. The protocol is compliant to RFC 3164. If you have external Linux server with syslogd service, use **"-r"** option to turn on the facility for receiving log from remote machine. You may also use some software that is available for Windows if it is RFC 3164 compliant.

Check **"Enable remote log"** and input the **"IP address"** and **"port"** number of the log server to enable the remote log facility.

In the **"Current log"**, the current system log file is displayed. The content of the log provides useful information about configuration and connection after system boot-up.

## Viewing system parameters

Click on this link on the configuration page to view the entire system's parameter settings.

# Maintenance

Four actions may be selected:

**Reboot:** Click the reboot button to restart system.

**Restore:** Click this to restore all settings to factory default except the settings in the "Network type" on the network page.

**Default:** Click on the Factory default button on the configuration page to restore the factory default settings. Any changes made thus far will be lost and the system will be reset to the initial factory settings. The system will restart and require the installation program to set up the network again.

**Upgrade firmware:** Select the firmware file and click upgrade button.

## Software revision upgrade

Customers can obtain up-to-date software from Vivotek's web site. An easy-to-use Upgrade Wizard is provided to upgrade the Network Camera with just a few clicks. The upgrade function is open to the Administrator only.

### To upgrade the system:

1. Download the firmware file named "xxx.pkg" from the appropriate product folder.
2. Run the Installation Wizard and proceed by following the prompts. Refer to the instructions of the Installation Wizard for details, or upgrade firmware from the HTTP web page directly.
3. The entire process will finish in a few minutes and will automatically restart the system.



If power fails during the writing process of Flash memory, the program in the memory of the Network Camera may be destroyed permanently. If the Network Camera cannot restart properly, ask your dealer for technical service.





# Appendix

## A. Troubleshooting

### Status LED

The following table lists the LED patterns in general:

Condition	LED color
Loading system after power on	Steady amber (green and blinking red)
During booting procedure	Steady amber
Detecting and setting network	Steady amber (green + red) until IP address is confirmed
After network is setup (system up)	Blinking green / amber every second and steady green
During the upgrade firmware process	Blinking green / amber every second and fast blinking red

### Reset and restore

There is a button at the back of the Network Camera. It is used to reset the system or restore the factory default settings. Sometimes resetting the system sets the system back to normal state. If the system problems remain after reset, restore the factory settings and install again.



Restoring the factory defaults will erase any previous settings. Reset or restore the system after power on.

**RESET:** Click on the button.

**RESTORE:**

1. Press on the button continuously.
2. Wait for self-diagnostic to run twice.
3. Free the button as soon as the second self-diagnostic starts.

## B. Technical specifications

### - System

CPU: VVTK-1000  
RAM: 64MB SDRAM  
ROM: 8MB FLASH ROM

### - Networking

#### Protocol

TCP/IP, HTTP, SMTP, FTP, DDNS, UPnP, Telnet, NTP, DNS, DHCP and RTSP

#### Physical

10 baseT or 100 baseT Fast Ethernet auto negotiation

### - Video

#### Algorithm supported

MPEG4(simple profile) for streaming video  
JPEG

#### Features

Adjustable image size, quality and bit rate  
Time stamp and text overlay  
3 motion detection windows  
5 privacy windows

#### Resolution

Motion JPEG video with resolution up to 640x480  
MPEG-4 video with resolution up to 640x480

### - Audio

AAC, GSM-AMR

### - Microphone

Internal microphone:  
Omni-directional  
Frequency: 50 – 16000Hz  
S/N ratio: more than 60dB

### - LED indicator

Dual color status indicator

### - Dimension

110mm(L) x 72mm(W) x 56mm(H)

### - Weight

NET. 315g

### - Power Supply

Input: 100-240VAC, 50/60Hz, 0.5A  
Output: 12VDC, 2A

### - Operating Environment

Temperature: 0-50°C/32-122°F  
Humidity: 95%RH

### - EMI & Safety

CE, FCC

### - Viewing system requirement

#### Operating system

Microsoft Windows 2000/XP

#### Browser

Internet Explorer 6.x or above  
Firefox 1.5.0.x or above

## **Technology License Notice**

### **AMR Technology**

This product includes AMR narrowband speech coding technology licensed by VoiceAge. Please refer to <http://www.voiceage.com/> for more details.

### **MPEG-4 AAC Technology**

This product includes MPEG-4 AAC audio coding technology licensed by Via Licensing. Please refer to <http://www.vialicensing.com/> for more details.

### **MPEG-4 Visual Technology**

This product includes one MPEG-4 encoder and one MPEG-4 decoder license. Installation of more than one decoder is prohibited. Please contact your reseller to purchase additional decoder licenses.

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NONCOMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USE AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLC. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

## **Electromagnetic Compatibility (EMC)**


This device complies with FCC Rules Part 15. Operation is subject to the following two conditions.

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

**USA** - This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a partial installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Shielded interface cables must be used in order to comply with emission limits.

**Europe**  - This digital equipment fulfills the requirement for radiated emission according to limit B of EN55022/1998, and the requirement for immunity according to EN50082-1/1992.

## **Liability**

Vivotek Inc. cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. Vivotek Inc. makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for any particular purpose.